

# Information technology — Security techniques — Digital signature schemes giving message recovery —

## Part 2: Mechanisms using a hash-function

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

# National foreword

This British Standard reproduces verbatim ISO/IEC 9796-2:1997 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

### Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

**Compliance with a British Standard does not of itself confer immunity from legal obligations.**

### Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO/IEC title page, pages ii to iv, pages 1 to 14 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 December 1998

© BSI 05-1999

ISBN 0 580 30926 6

### Amendments issued since publication

| Amd. No. | Date | Comments |
|----------|------|----------|
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |

# Contents

|                        | Page               |
|------------------------|--------------------|
| National foreword      | Inside front cover |
| Foreword               | iii                |
| Text of ISO/IEC 9796-2 | 1                  |



# INTERNATIONAL STANDARD

**ISO/IEC  
9796-2**

First edition  
1997-09-01

---

---

## **Information technology — Security techniques — Digital signature schemes giving message recovery —**

### **Part 2: Mechanisms using a hash-function**

*Technologies de l'information — Techniques de sécurité — Schémas de  
signature numérique rétablissant le message —*

*Partie 2: Mécanismes utilisant une fonction de hachage*



Contents

|                                                                            | Page |
|----------------------------------------------------------------------------|------|
| Foreword                                                                   | iii  |
| Introduction                                                               | 1    |
| 1 Scope                                                                    | 1    |
| 2 Normative references                                                     | 2    |
| 3 Terms and definitions                                                    | 2    |
| 4 Symbols and abbreviations                                                | 3    |
| 5 Requirements                                                             | 4    |
| 6 Signature process                                                        | 5    |
| 7 Verification process                                                     | 6    |
| Annex A (informative) Example of a public-key system for digital signature | 8    |
| Annex B (informative) Illustrative examples related to Annex A             | 9    |
| Figure 1 — Signature process                                               | 5    |
| Figure 2 — Verification process                                            | 6    |
| Table 1 — Structure of the intermediate string $S_i$ ( $k$ bits)           | 7    |

**Descriptors:** Data processing, information interchange, messages, protection of information, security techniques, digital signatures.

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 9796 consists of the following parts, under the general title *Information technology — Security techniques — Digital signature schemes giving message recovery*.

— *Part 1: Mechanisms using redundancy;*

— *Part 2: Mechanisms using a hash-function.*

International Standard ISO/IEC 9796-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*.

Annex A and Annex B of this part of ISO/IEC 9796 are for information only.

